MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 3, 2015/2016

TMI 3231 - MALWARE AND INTRUSION DETECTION

(All sections / Groups)

2 JUNE 2016
9:00 a.m – 11 a.m
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This Question paper consists of 6 pages with 6 Questions only.
2. Attempt **FIVE** out of **SIX** questions. All questions carry equal marks and the distribution of the marks for each question is given.
3. Please print all your answers in the Answer Booklet provided.

QUESTION 1

a) As a security professional in a company, you have been receiving multiple reports on identifying Web Trojans in your company. To be able to countermeasure against such attacks, a thorough understanding of their mechanism is necessary. Demonstrate the steps common in a successful Web Trojan attack.

(3 marks)

b) Explain how rootkits can contribute in increasing the catastrophic effects of malware.

(2 marks)

c) Risk is the state of being unsecure, either partially or totally. Do you think it is logical to state that organizations can completely eliminate risks? Explain your answer. Suggest TWO (2) measures to control risk.

(3 marks)

d) How can you apply the concept of "balancing Information Security and Access" in designing the architecture and setting the security measures of your network? Elaborate your answer by providing an example.

(2 marks)

QUESTION 2

a) Differentiate the detection methods in second (heuristic scanners) and third (activity traps) generation antiviruses.

(2 marks)

Continued...

b) Caching data and VPN are two advanced security functions that are offered by some firewalls. If you purchase a firewall that provides these functions, explain the roles of each of these functions in your company's computer network.

(4 marks)

c) Social engineering is one of the most popular forms of attacks. Identify TWO (2) social engineering tactics that can be used to target bank customers (including online banking customers) and demonstrate the best measure to protect against social engineering attacks.

(4 marks)

QUESTION 3

a) Point out a main advantage of the stateful packet filters over the stateless packet filters.

(2 marks)

b) Application proxies can be mainly set up in two different architectures/settings. Elaborate each of these architectures and highlight ONE (1) advantage and ONE (1) disadvantage of each.

(4 marks)

c) As a security specialist, you have installed a single firewall to protect your company's network. Your company has introduced a new attractive product and allows online shopping from its website. Therefore, your network traffic has been substantially increased and caused your firewall to be overloaded with a high volume of traffic and led to slowing down your network. You are willing to purchase additional firewalls to address the problem. Explain how the concept of load balancing and load sharing could help you in addressing this issue.

(4 marks)

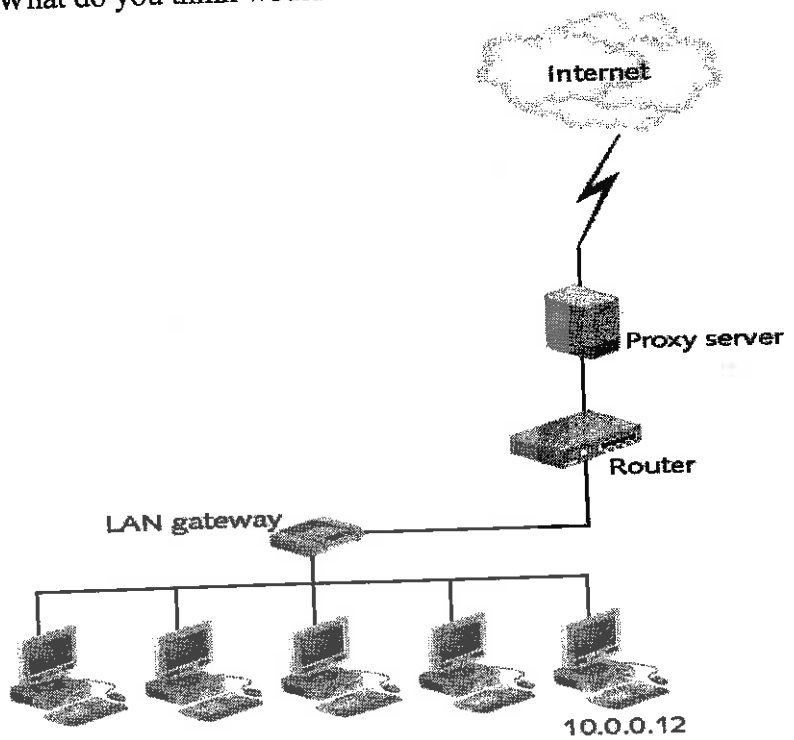
Continued...

QUESTION 4

a) As a security professional, you have recommended replacing the current packet filtering firewalls in your network with proxy servers. Suppose this task requires a considerable budget, express FOUR (4) reasons that proxy servers provide better security comparing to packet filter firewalls to obtain the approval of the top management.

(4 marks)

b) The figure below illustrates a network architecture with a proxy server. Assume that the host with IP address 10.0.0.12 wants to request a webpage from the internet. Explain the steps taken by proxy server to establish the connection between the local host and an external host. What do you think would be the main disadvantage of using proxy servers?



(4 marks)

Continued...

c) Your company is specialized in producing pharmaceutical products and the nature of your work requires you to send your company's representatives to all parts of Southeast Asia. Imagine your representatives have very little knowledge about computers and you have decided to improve the security of your company. You can choose between transparent and non-transparent proxies. Which option is less likely to cause work overhead and issues for your system administrator and your company's representatives? Why?

(2 marks)

QUESTION 5

a) Your company has provided you with a smart phone (mobile phone) in order to be able to carry out some of your tasks while travelling. Therefore, aside from your personal data (messages, contact, and images); you are to store your company's sensitive information on your phone. Propose THREE (3) measures that can contribute to your smart phone's security.

(3 marks)

b) It is recommended NOT to use Network Address Translation (NAT) with IPsec. Can you elaborate the reason for this recommendation? What could happen if you use NAT with IPsec?

(2 marks)

c) Company XYZ has decided to use MAC filtering in order to improve it security. Explain how MAC filtering firewalls work and highlight their main weakness.

(2 marks)

d) Do you use ad-hoc mode or infrastructure mode in your home wireless network? Explain how changing your default SSID can improve the security of our wireless network.

(3 marks)

Continued...

QUESTION 6

a) You have been hired by multi-branched financial company which deals with highly sensitive data about customer's assets and monetary transactions. Discuss TWO (2) domains/applications that using cryptography controls could improve the overall security of your company.

(2 marks)

b) XYZ Company has decided to place all its servers in one branch and make use of VPN to connect to servers from other branches. Explain TWO (2) advantages and TWO (2) disadvantage of this approach.

(4 marks)

c) The nature of your company requires its agents which are frequently travelling abroad to be able to get connected to the servers in the company (to upload and download information). As a security specialist you are to configure the laptop of each agent to be able to use VPN when connecting to company's servers. Elaborate TWO (2) main points that you need to consider when configuring their laptops.

(2 marks)

d) Alice and Bob use asymmetric key cryptography to securely communicate with each other. The file that contains the Alice's private key is corrupted. Therefore, Alice does not have access to her private key anymore.

a. Can Alice still encrypt messages to Bob? Explain your answer.

b. Can Alice still verify signatures issued by Bob? Explain your answer.

(2 marks)

End of Page.